Microsoft

# Microsoft Digital Defense Report

## Building and improving cyber resilience

October 2023
Microsoft Threat Intelligence

# Contents

The data, insights, and event in this report are from July 2022 through June 2023 (Microsoft fiscal year 2023), unless otherwise noted.

For easier viewing and navigating through the report on certain browsers, we suggest using Adobe Reader, which is available for free on the Adobe website.

Chapter 1
**Introduction**

Introduction 3
Sharing Microsoft's unique vantage point 5
The power of partnership in building cyber resilience 6
How can we protect against 99% of attacks? 7
Driving global progress through the Cybersecurity Tech Accord 8
About this report 9
Threat actor map 11

Chapter 2
**The State of Cybercrime**

Key developments 13
Introduction 14
How the threat landscape is evolving 15
Insights on ransomware and extortion 17
Insights on phishing 27
Insights on business email compromise 32
Insights on identity attacks 34
Insights on distributed denial of service attacks (DDoS) 38
Return on mitigation: Targeting investment to increase resilience 41

Chapter 3
**Nation State Threats**

Key developments 46
Introduction 47
Russia 54
China 60
Iran 65
North Korea 70
Palestinian threat actors 73
The emerging threat posed by cyber mercenaries 74

Chapter 4
**Critical Cybersecurity Challenges**

Key developments 76
Introduction 77
The state of IoT and OT security 78
Improving global critical infrastructure resilience 86
Innovating for supply chain resilience 90

Chapter 5
**Innovating for Security and Resilience**

Key developments 97
Introduction 98
Using the power of AI for cybersecurity 100
Working together to shape responsible AI 106

Chapter 6
**Collective Defense**

Key developments 109
Introduction 110
How the global Cybercrime Atlas will revolutionize cybercrime intelligence and collaboration 111
Collective intelligence and defense against Volt Typhoon 112
Uniting forces against cybercrime: A success story of collaboration and disruption 113
Advancing open source security together 116
Strengthening media content provenance, accountability, and transparency 117
Combining efforts to safeguard democracy 118
How we are addressing the digital talent and diversity shortage 119
The CyberPeace Institute: Uniting to empower nonprofits with cyber resilience 121
Building cybersecurity capacity through the Cyber Development Goals 122

Appendix
**Additional information**

Cybersecurity Tech Accord principles mapping index 124
Contributing teams 126
Footnotes 128

# Chapter 1 Introduction

## About this report


| | |
|---|---|
| Introduction | 3 |
| Sharing Microsoft's unique vantage point | 5 |
| The power of partnership in building cyber resilience | 6 |
| Driving global progress through the Cybersecurity Tech Accord | 8 |
| About this report | 9 |
| Threat actor map | 11 |

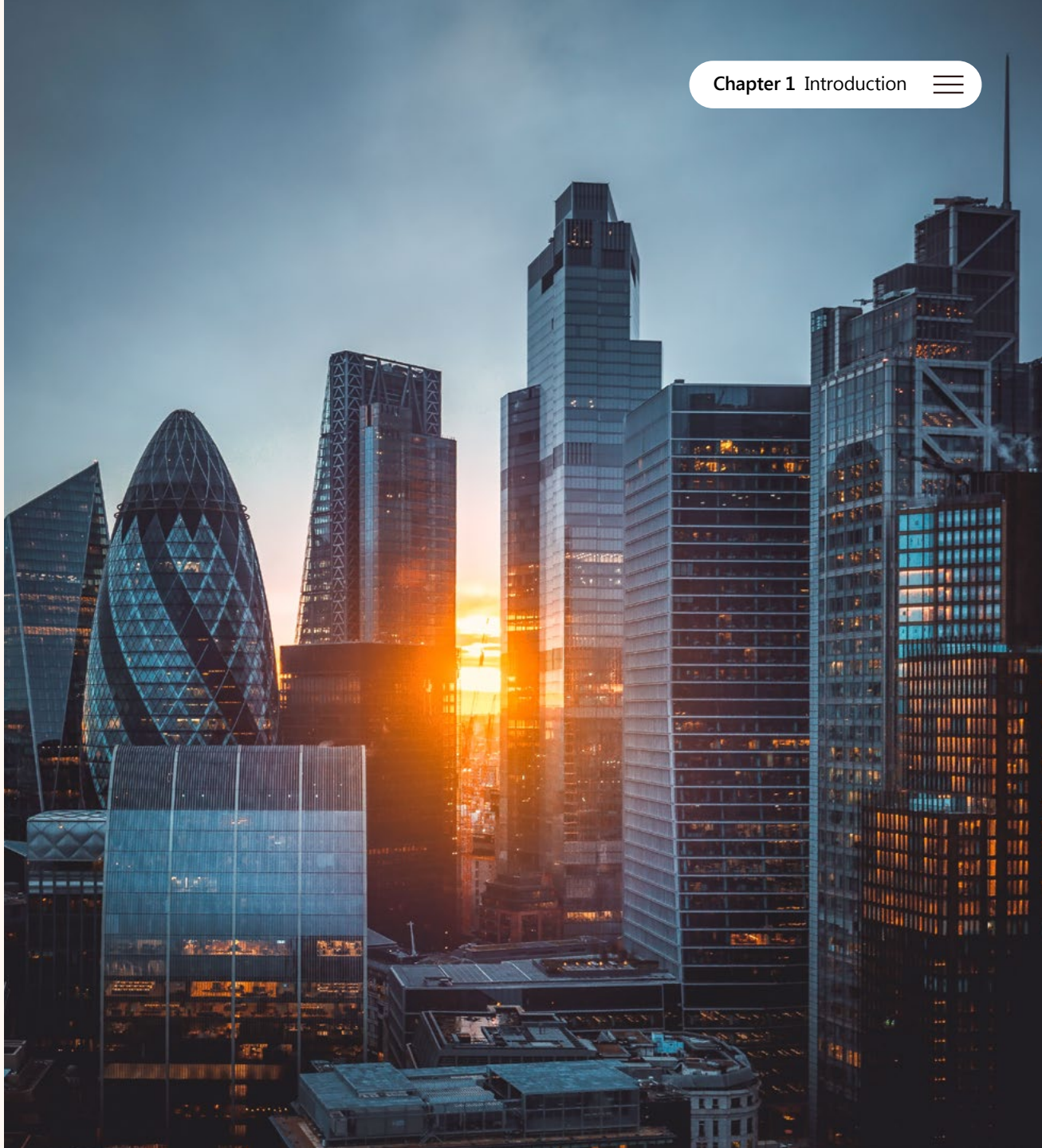

# Securing our future together

## Introduction from Tom Burt

Over the last year, threats to digital peace have reduced trust in technology and highlighted the urgent need for improved cyber defenses at all levels. Encouragingly, defenders the world over are responding to the call to improve security with the public and private sectors investing and collaborating to confront the challenges and build long-term resilience.

In this fourth annual edition of the Microsoft Digital Defense Report, we draw on our unique vantage point to share insights on how the threat landscape has evolved and discuss the shared opportunities and challenges we all face in securing a resilient online ecosystem which the world can depend on.

"Close collaboration between the public and private sectors to formulate, enforce, and harmonize these requirements is crucial to improve global cybersecurity and foster innovation."



"As the digital domain faces new and more threatening challenges, defenders are being driven to innovate and collaborate more closely than ever."

As the digital domain faces new and more threatening challenges, defenders are being driven to innovate and collaborate more closely than ever. For example, Russia's use of cyberweapons as part of its hybrid war against Ukraine sparked sustained collaboration between Microsoft and Ukrainian officials to successfully defend against most of these cyberweapons.

Russia is not alone in its use of destructive malware; we have also seen increased use of cyberweapons by Iran to pressure the Albanian government and in its ongoing conflict with Israel. At the same time, nation states are becoming increasingly sophisticated and aggressive in their cyber espionage efforts, led by highly capable Chinese actors focused on the Asia Pacific region in particular.

One recent example of the troubling increase in aggression and capability involves a Chinese actor, which Microsoft calls Volt Typhoon. It used inventive tradecraft to infiltrate and pre-position malware in the networks of a range of communications companies and other critical infrastructure organizations in Guam and the United States, deploying "living off the land" techniques to evade detection.

Nation-state actors were not alone in stepping up their abuse of the digital ecosystem. Well-resourced cybercriminal syndicates also continue to grow and evolve, leveraging the cybercrime-as-a-service ecosystem we highlighted last year. Ransomware-as-a-service and phishing-as-a-service are key threats to businesses and cybercriminals have conducted business email compromise and other cybercrimes, largely undeterred by the increasing commitment of global law enforcement resources.

Many vendors are taking steps to improve the cybersecurity of their products and services, developing new tools to help customers better defend against attackers. Governments across the globe are providing the public with more information about cyber threats and how to counter them, like the effective alerts from the US Cybersecurity and Infrastructure Security Agency's (CISA) Shields Up campaign. Governments are also imposing new legal and regulatory requirements for cybersecurity. While many of these are beneficial, they can impose counterproductive conditions—such as requiring overly rapid reporting of cybersecurity incidents or establishing inconsistent or conflicting requirements across agencies or geographies. Close collaboration between the public and private sectors to formulate, enforce, and harmonize these requirements is crucial to improve global cybersecurity and foster innovation.

As we are seeing, Artificial Intelligence (AI) technologies are set to become a major focus of regulators and industry. We will undoubtedly see attackers using AI as a tool to refine phishing messages, develop malware and enable other abuses of technology. But AI will also be a critical component of successful defense. For example, in Ukraine we saw the first successful use of AI technology to help defend against Russian cyberattacks. In the coming years, innovation in AI-powered cyber defense will help reverse the tide of cyberattacks.

Advancing the promise of digital peace requires public-private collaboration to ensure we are bringing to bear the best technological and regulatory tools to combat cyber aggression. We need more and deeper alliances in the private sector and stronger partnerships between the private and public sectors. Enabling this collaboration can be challenging but, when successful, it drives meaningful impact. We must accelerate the move of critical computing workloads to the cloud, where vendors' security innovations will be most impactful, and ensure AI innovation provides defenders with the durable technological advantage over attackers that it promises.

**Tom Burt**
Corporate Vice President, Customer Security & Trust

# Sharing Microsoft's unique vantage point

Cybersecurity is a defining challenge of our time. Organizations of every size across every industry around the globe feel the urgency and pressure of protecting and defending against increasingly sophisticated attacks.

While AI is transforming cybersecurity, using it to stay ahead of threats requires massive amounts of diverse data. Here at Microsoft, our more than 10,000 security experts analyze over 65 trillion signals each day with the help of AI, and Microsoft Threat Intelligence teams track hundreds of threat actor groups worldwide. The Microsoft security ecosystem includes more than 15,000 security partners with specialized solutions, while the global open community of security researchers and testers contribute to bug bounties and security challenges. This broad, deep, and diverse security ecosystem is driving some of the most influential insights in cybersecurity. Together, we can build cyber resilience through innovative action and collective defense.

**As part of our longstanding commitment to create a safer world, Microsoft's investments in security research, innovation, and the global security community include:**

## 65 trillion
signals synthesized daily

That is over 750 million signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

## 10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

## 4,000
identity attacks blocked per second

4,000 identity authentication threats blocked per second.

## 15,000+
partners in our security ecosystem

15,000+ partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

## 300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

## 100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

## 135 million
managed devices

135 million managed devices providing security and threat landscape insights.

All data is based on Microsoft fiscal year 2023 unless otherwise indicated.

# The power of partnership in building cyber resilience

We believe every individual and company around the world should be empowered to meet its security needs. Achieving this will require a collective global effort as we harness the power of partnership to strengthen our defenses together.

Strength in numbers. Stronger together. Together we stand. Societies around the world recognize the benefits of collective behavior. The power of multistakeholder partnerships in cybersecurity, too, cannot be ignored as we seek to answer the question, "What we can do to ensure a more safe and secure world for everyone on the planet?"

Individual organizations are often focused on safeguarding their own data and systems and protecting their customers, constituents, and communities.

But partnerships act as a force multiplier for everyone involved in cybersecurity. Collaborative efforts among stakeholders—including government agencies, private sector entities, academia, non-profits, and other organizations—are crucial in building resilient defenses against cyber threats.

### The cyber poverty line

To understand the need for collaboration, it is useful to consider the concept of a "cyber poverty line." In the same way that governments and economists establish a social poverty line to determine a bare minimum standard of living, the cyber poverty line is the minimum level of resources required for adequate protection from cyber threats. As we ponder the implication of the existence of a cyber poverty line, important questions begin to surface. How, exactly, do we quantify the cyber poverty line? Who is below it and how can we work together to support them to rise above it? These questions underscore the imperative of partnership in cybersecurity and serve as the genesis of meaningful conversations we must have.

### Public-private partnerships, policy, and standards

The opportunities for partnership across the public and private sectors, policy organizations, and standards bodies are multi-dimensional. From ensuring the technology community is building safer, more secure technology and collaborating on threat intelligence and trends to developing common standards to take down and block the tools cybercriminals use, strong and bi-directional partnerships between organizations are crucial.

As much as any individual company's shareholders would like it to be so, no one technology company can solve or overcome every cybersecurity challenge. Partnerships across the technology community are an absolute necessity to ensure organizations of all types and sizes, in every industry and region, can protect themselves. This means working together to push the boundaries of innovation, ensuring technical integration of products in the security space and addressing the end-to-end security needs of customers.

> The concept of a cyber poverty line allows us to identify the minimum level of resources required for adequate protection from cyber threats and who we must support to rise above it.

### Non-profit, academia, and research

Non-profit, academia, and research organizations play a crucial role in advancing cybersecurity. By collaborating with industry partners, they bridge the gap between theoretical knowledge and practical application. Academic institutions contribute to cybersecurity research, develop innovative technologies, and educate the next generation of cybersecurity professionals. Collaborative research projects and initiatives between academia, non-profits, and industry promote innovation and help tackle emerging cyber threats effectively.

It is essential that stakeholders recognize their shared responsibility and actively engage in partnerships that enhance cybersecurity. History has already shown that by working together, we can build a safer digital future for individuals, organizations and nations—but there is so much more to be done.

**For more about the power of partnerships, please see the Collective Defense chapter on page 108.**

**Additional information**

Collaboration is crucial to strengthening cybersecurity | Microsoft On the Issues

# How can we protect against 99% of attacks?

While we explore the many dimensions of the cyber threat landscape, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
   - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
   - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.
   - Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

## Fundamentals of cyber hygiene

**99%**

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]

# Driving global progress through the Cybersecurity Tech Accord

Since its inception, the Cybersecurity Tech Accord has witnessed remarkable progress. As we mark its fifth anniversary, we celebrate a groundbreaking commitment by 156 technology and security companies from around the world to protect our customers from malicious attacks by cybercriminals and nation states.

The Cybersecurity Tech Accord has worked to be the technology industry's voice on matters of peace and security in cyberspace and to uphold a commitment to protect users and customers everywhere from evolving cyber threats. At the core of this historic initiative are four fundamental cybersecurity principles:

1. Better defense: We will protect all of our users and customers everywhere.
2. No offense: We will oppose cyberattacks on innocent citizens and enterprises from anywhere.
3. Capacity building: We will help empower users, customers, and developers to strengthen cybersecurity protection.
4. Collective action: We will partner with each other and likeminded groups to enhance cybersecurity.

The Accord has launched several initiatives, including the Internet of Things (IoT) Security Resource Hub, which aims to establish a strong global baseline for IoT security in the next generation of consumer products. Signatories and industry partners have also embraced a set of principles to combat the menace of cyber mercenaries. The group also engages in extensive consultations with governments, civil society, and private sector partners, advocating for responsible nation-state behavior and amplifying the technology industry's role in international cybersecurity.

In the past year, the Cybersecurity Tech Accord has made strides in raising awareness of the escalating threats posed by some nation-state actors. In particular, the group launched an Annual State of International Cybersecurity Thermometer, which in 2023 reached a "boiling point," largely due to the widespread and unprecedented use of cyber operations in the armed conflict in Ukraine.

The Cybersecurity Tech Accord has invested in promoting diversity, particularly empowering women in cybersecurity. Microsoft is proud to work with industry partners and non-profit organizations worldwide to broaden access and foster the careers of women working in this critical field.

**To understand how topics discussed in this report track against the Cybersecurity Tech Accord, please see page 124.**

**Additional information**

https://cybertechaccord.org


In 2023, the cyber conflict thermometer reached "the boiling point"

# About this report

### Signposts

For ease of reading, we have included icons to signpost discussion that relates to specific efforts throughout this report. This relates to AI-related content, partnerships, and the Cybersecurity Tech Accord principles.

### Cybersecurity Tech Accord principles:

Icons representing the principles of the Cybersecurity Tech Accord are signposted throughout this report to serve as a visual reminder of our collective dedication to safeguarding the digital landscape. A full index is provided on page 124.

- Pr Protect Users and Customers
- Op Oppose Cyberattacks
- Em Empower Users, Customers, and Developers
- Pa Partner to Enhance Cybersecurity

**Scope:** Unless otherwise noted, this report covers the period from July 2022 through June 2023 (Microsoft fiscal year 2023).

In general, when referring to critical infrastructure sectors in this report, we are including the 16 sectors identified by the US Cybersecurity & Infrastructure Security Agency (CISA)[2]:

- Chemicals
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater

### Last year's report

The 2022 Digital Defense Report focused on illuminating the threat landscape and empowering a digital defense. Relevant discussion from last year is referenced in this report.


You can access the 2022 Microsoft Digital Defense Report in the archive section at https://aka.ms/mddr.

# Threat actor descriptions and naming

Throughout this report, we refer to the five key groups that Microsoft uses to characterize threat actors:

- **Nation-state actors** are cyber operators who act on behalf of, or directed by, a nation/state-aligned program, irrespective of whether the goal is espionage, financial gain, or retribution.
- **Financially motivated actors** are cyber campaigns/groups directed by a criminal organization/person with the motivation of financial gain which have not been associated with high confidence to a known non-nation state or commercial entity.
- **Cyber mercenaries or private sector offensive actors** refer to commercial actors that are known/legitimate legal entities that create and sell cyberweapons to customers who select targets and operate the cyberweapons.
- **Influence operations** are manipulative information campaigns communicated online or offline that are intended to shift perceptions, behaviors, or decisions by target audiences to further a group or a nation's interests and objectives.
- **Groups in development** is a temporary designation given to an unknown, emerging, or developing threat activity. This allows Microsoft to track it as a discrete set of information until we can reach high confidence about the origin or identity of the actor behind the operation.

### Threat actor naming taxonomy

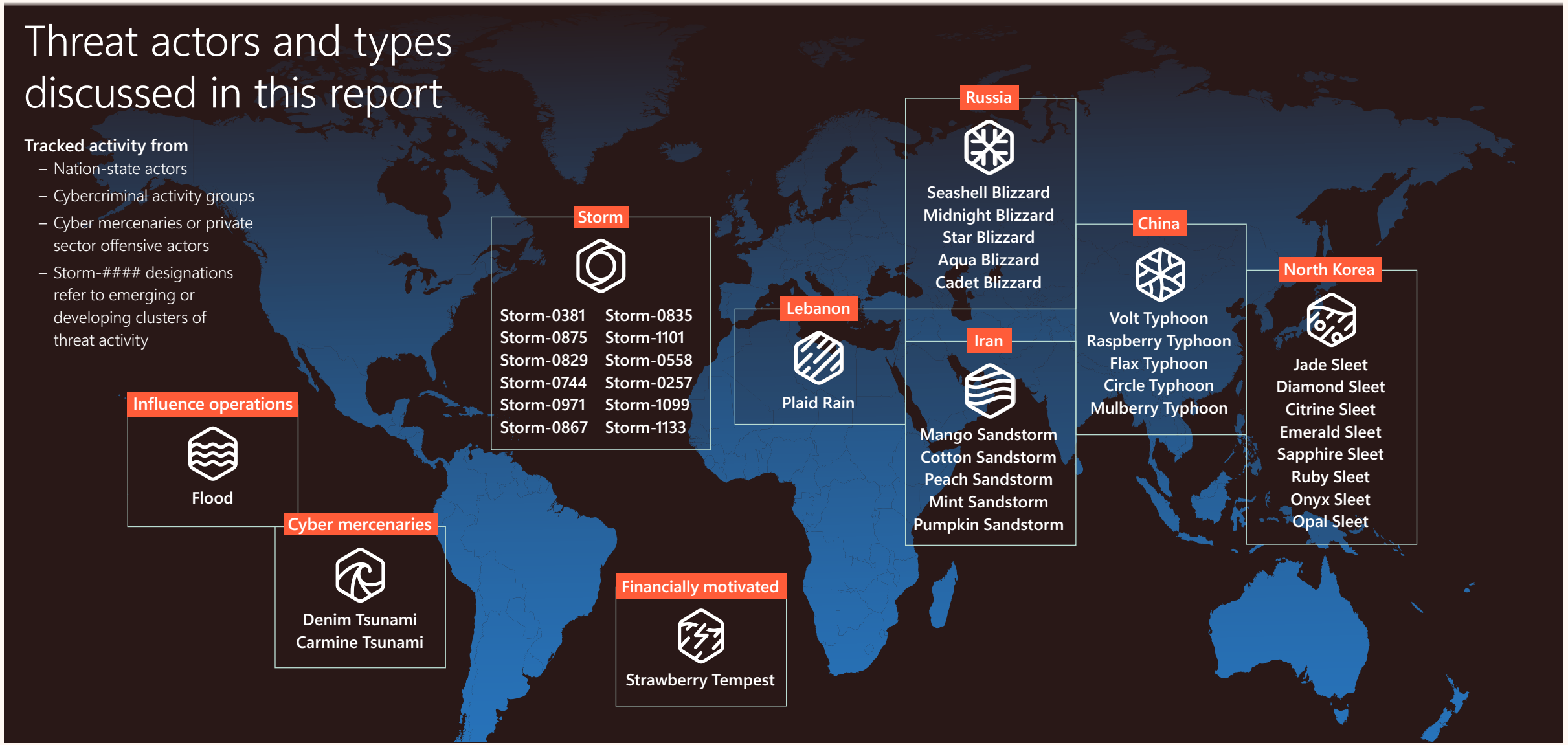
In April, we announced that we have shifted to a new threat actor naming taxonomy aligned to the theme of weather. The complexity, scale, and volume of threats is increasing, driving the need to reimagine not only how Microsoft talks about threats but also how we enable customers to understand those threats quickly and with clarity. With the new taxonomy, we intend to bring better context to customers and security researchers that are already confronted with an overwhelming amount of threat intelligence data. It will offer a more organized, memorable, and easy way to reference adversary groups so that organizations can better prioritize threats and protect themselves. Simply put, security professionals will instantly have an idea of the type of threat actor they are up against, just by reading the name.

#### Additional information

How Microsoft names threat actors | Microsoft

### Other definitions:

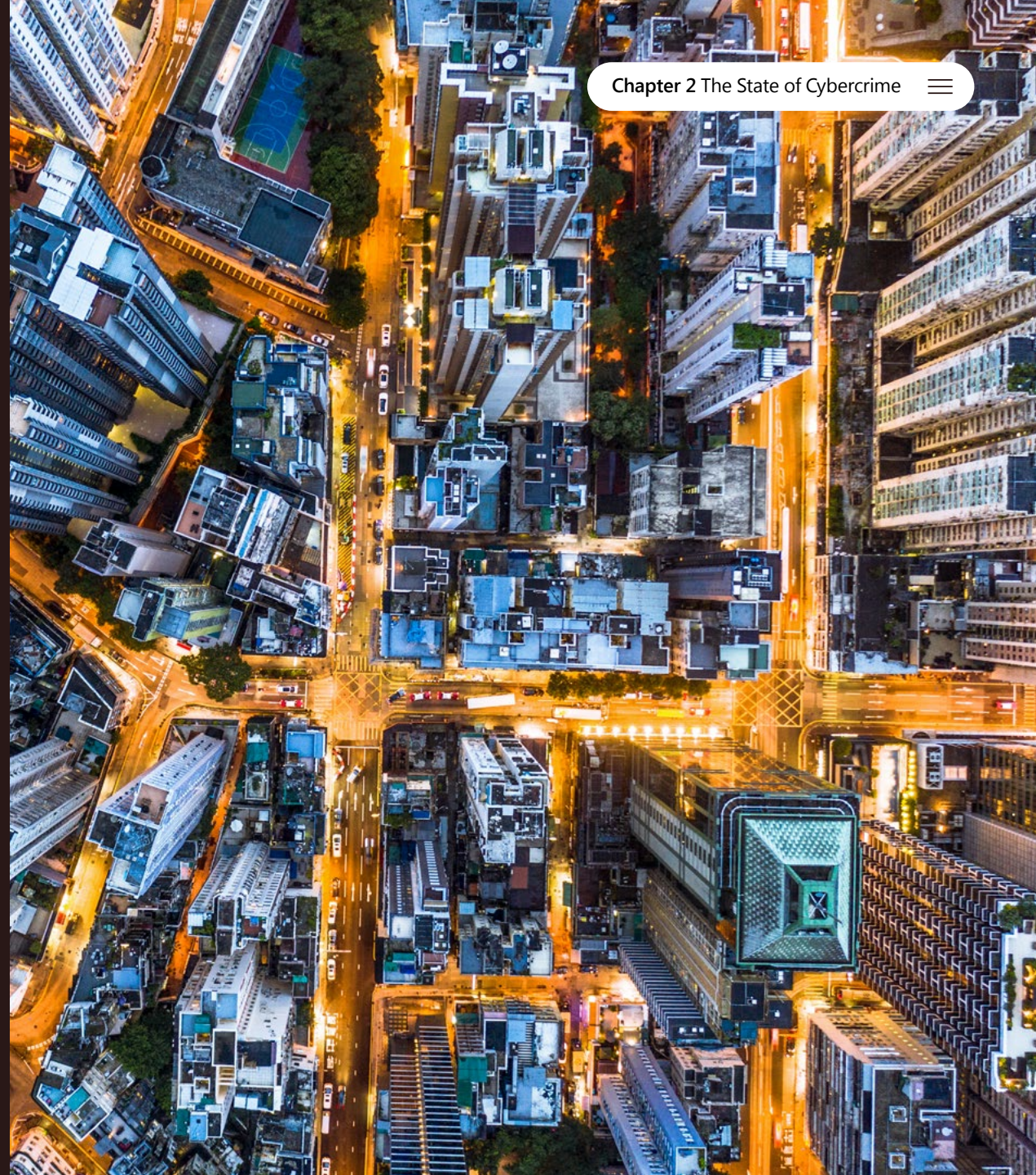
- **Cyber-enabled influence operations:** Operations that combine offensive computer network operations with messaging and amplification in a coordinated and manipulative way to shift perceptions, behaviors, or decisions by target audiences to further a group or nation's interests and objectives.
- **NSN data:** This data is based on aggregated nation-state notifications (NSNs)—notices that we send to customers when they have been targeted or compromised by a nation-state actor that is tracked by Microsoft. Data overwhelmingly reflects activity against Office 365, followed by Outlook and Hotmail. We count NSN data by number of targeted organizations.
- **Events data:** This data covers a broader range of investigative observations of nation-state threat actor activity than NSNs. Activity captured in "events" ranges from reconnaissance and movement on network to data exfiltration or deletion.


Threat actors and types discussed in this report
Tracked activity from
– Nation-state actors
– Cybercriminal activity groups
– Cyber mercenaries or private sector offensive actors
– Storm-#### designations refer to emerging or developing clusters of threat activity
Influence operations
Flood
Cyber mercenaries
Denim Tsunami
Carmine Tsunami
Storm
Storm-0381
Storm-0875
Storm-0829
Storm-0744
Storm-0971
Storm-0867
Storm-0835
Storm-1101
Storm-0558
Storm-0257
Storm-1099
Storm-1133
Lebanon
Plaid Rain
Financially motivated
Strawberry Tempest
Russia
Seashell Blizzard
Midnight Blizzard
Star Blizzard
Aqua Blizzard
Cadet Blizzard
Iran
Mango Sandstorm
Cotton Sandstorm
Peach Sandstorm
Mint Sandstorm
Pumpkin Sandstorm
China
Volt Typhoon
Raspberry Typhoon
Flax Typhoon
Circle Typhoon
Mulberry Typhoon
North Korea
Jade Sleet
Diamond Sleet
Citrine Sleet
Emerald Sleet
Sapphire Sleet
Ruby Sleet
Onyx Sleet
Opal Sleet

# Chapter 2
# The State of Cybercrime

## What we know about cybercrime today


| | |
|---|---|
| Key developments | 13 |
| Introduction | 14 |
| How the threat landscape is evolving | 15 |
| Ransomware and extortion | 17 |
| Phishing | 27 |
| Business email compromise | 32 |
| Identity attacks | 34 |
| Distributed denial of service attacks (DDoS) | 38 |
| Return on mitigation: Targeting investment to increase resilience | 41 |

The State of Cybercrime

# Key developments

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands on keyboard attacks, using living-off-the-land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

80-90%

**of all successful ransomware compromises originate through unmanaged devices.**

Find out more on page 18

**A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.**

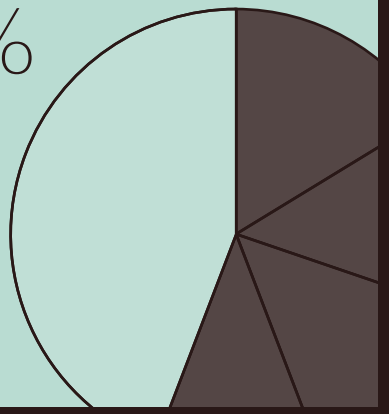
Find out more on page 41

70%

of organizations encountering human-operated ransomware had fewer than 500 employees.

Find out more on page 18

Human-operated ransomware attacks are up more than 200%



Find out more on page 17

Password based attacks spiked in 2023

Find out more on page 34

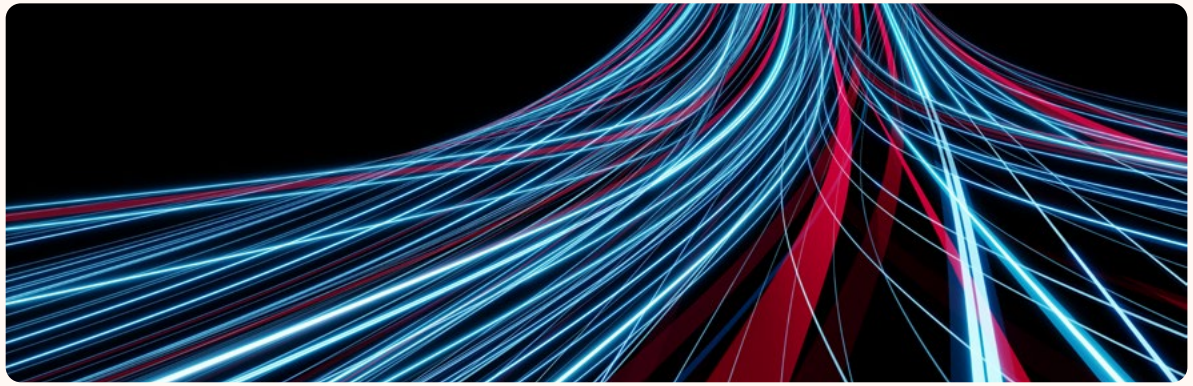
Last year marked a significant shift in cybercriminal tactics

**with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.**

Find out more on page 39

# Joining forces against cybercrime

## Introduction from Amy Hogan-Burney



While cybercriminals have remained hard at work, we are seeing public and private sectors come together to disrupt the technologies criminals use, hold them to account, and support the victims of cybercrime.

As cybercriminals look for new ways to generate income, they have stayed focused on exploiting weakness in humans and technology, staying ahead of security measures, and coordinating to create sophisticated global networks that sell services. To combat them, public and private sector professionals and organizations are creating strong partnerships that are disrupting criminal's technology, hold threat actors accountable, and increase resilience to attacks.

As a result, attackers are finding themselves in the crosshairs of law enforcement. Many have been outed, including the Conti ransomware operator known as "Target" whose unmasking includes a $10 million reward for additional information, indicted (Yevgeniy Polyanin) or arrested (Yaroslav Vasinskyi) alleged to have deployed the Sodinokibi/REvil ransomware to attack businesses and governments.

Governments are also looking beyond criminals to rescue victims, disrupt malicious technology, and seize and return money–as was seen in the case of the Hive ransomware. The private sector is an essential partner in these efforts, whether through criminal referrals and information sharing with law enforcement or through technical and legal action, as seen in Microsoft and Fortra's action to disrupt cracked, legacy copies of Cobalt Strike and abused Microsoft software see page 113.

Op Cybersecurity Tech Accord principles mapping index on **page 124**

The result is that cybercriminals are looking for ways to increase their anonymity and effectiveness. As human-operated ransomware attacks on small and medium businesses increase, we have seen more use of remote monitoring and management tools that leave behind less evidence. Many of these ransomware attacks attempt to compromise or gain access to unmanaged or bring-your-own devices because they typically have fewer security controls and defenses.

Attackers continue to look for the easiest method to gain unauthorized access to any system through identity attacks such as traditional brute-force attempts, sophisticated password spray attempts across multiple countries and IP addresses, and adversary-in-the middle (AiTM) attacks. Phishing is not going away, and attackers are using both malware phishing to compromise devices and AiTM phishing to steal identities that can be used in further criminal activity such as business email compromise.

As you read this report, I encourage you to look for opportunities to improve your defensive security posture, identify areas where you may need investment, and explore ways to make training programs more effective. Consider your opportunities to engage in simulated cyberattacks or tabletop exercises, invest in threat intelligence and actor tracking in the cybercrime space, share information with law enforcement, and take technical or legal disruptive actions. We all have a part to play in fighting cybercrime, and I urge you to consider what more you, your company, or your government could do to help improve cyber resilience.

**Amy Hogan-Burney**
General Manager, Associate General Counsel, Cybersecurity Policy & Protection

# How the threat landscape is evolving

The cyber threat landscape is continuing to evolve toward more effective and more damaging attacks, which often take place at scale. According to our data, organizations faced an overall increase in ransomware attacks compared to the previous year, while the number of human-operated ransomware attacks almost tripled.

13%

of human-operated ransomware attacks that moved into the ransom phase included some form of data exfiltration.

This was accompanied by a sharp increase in the use of remote encryption during attacks. Using this method, an attacker encrypts a file on a different computer, and then sends the encrypted file to the original computer. This can happen if one computer on a network is hacked and has access to another computer with the compromised user account(s). No additional software is needed on the original computer, and no harmful files are left behind.

Data extortion is also on the rise. Since November 2022, we observed a doubling of potential data exfiltration instances–the theft or unauthorized removal or movement of data from a device. Thirteen percent of human-operated ransomware attacks that moved into the ransom phase had some form of data exfiltration.

The frequency of business email compromise (BEC) attacks has skyrocketed to over 156,000 daily attempts. Microsoft Entra data shows attempted password attacks increased more than tenfold in 2023, from around 3 billion per month to over 30 billion. This translates to an average of 4,000 blocked attacks per second targeting Microsoft cloud identities.

# What we can learn from attack notifications

Managed extended detection and response (XDR) services, such as Microsoft Defender Experts, are invaluable resources for security operations centers to effectively detect and respond to critical incidents.

When we observe novel tactics, techniques, and procedures, human-directed attacks, or attack progression, notifications are sent to our customers to provide specific information regarding the scope, method of entry, and instructions for remediation.

Pr Cybersecurity Tech Accord principles mapping index on **page 124**

**Based on the notifications shared with customers, these are the top threats identified by Microsoft Defender Experts this year:**

1. **Successful identity attacks:** Attacks across identity included traditional brute-force attempts, sophisticated password spray attempts across multiple countries and IP addresses, and adversary-in-the middle (AiTM) attacks.

   **For more about identity attacks, see page 34**.

2. **Ransomware encounters:** These are defined in this report as any instance of ransomware activity or attempted attacks that we have detected and prevented or alerted on, throughout the various stages of a ransomware attack.

   In addition to several ransomware variants this year, we observed a unique large-scale ransomware campaign targeting both endpoints and cloud architecture of an organization. This was driven by the threat actor we named Mango Sandstorm. This campaign included both on-premises and cloud environments, and involved privilege escalation and destruction activities, including deletion of victim user resources, and persistence using OAuth applications. Attackers added a secret or certificate to an application in order to connect to Azure Active Directory (Azure AD) as the application, and perform operations (such as reading confidential data and emails, exfiltrating information through emails) leveraging the application permissions that are assigned to it.

   **For more about ransomware see page 17**.

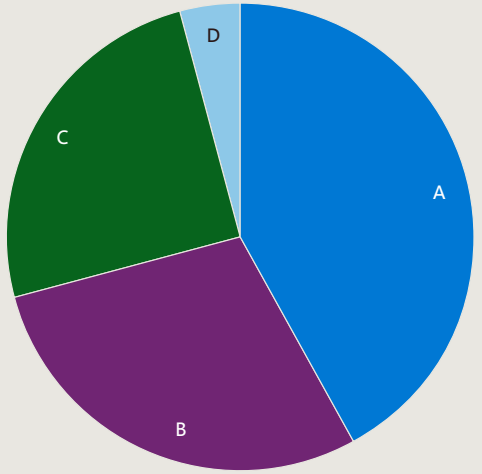
3. **Targeted phishing attempts leading to device or user compromise:** We have observed both malware phishing with intent to compromise devices, and AiTM phishing attempting to steal identities. Defense evasion techniques included phishing from compromised vendors and abuse of legitimate services.

   **For more about phishing and AiTM, see page 27**.

4. **Business email compromise (BEC):** Attackers used various methods including email conversation hijacking and mass spamming with malicious applications to commit financial fraud. They also sent phishing emails with harmful links and attachments from the victim's email address to other users within the victim's organization. Since these phishing emails were sent internally, multiple users fell victim to the attack by clicking on the links within a short period of time.

   **For more about BEC, see page 32**.

**Distribution of top four attack progression notifications**




A 42% Successful identity attacks

C 25% Successful targeted phishing attempts

B 29% Ransomware encounters

D 4% Business email compromise (BEC)

Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

**Additional information**

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft

Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity | Microsoft

# Insights on ransomware and extortion

## New tactics and trends

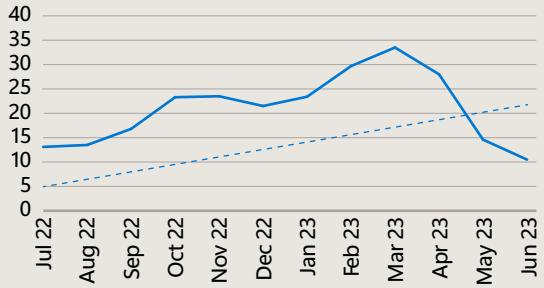
Microsoft's telemetry indicates that organizations faced an increased rate of ransomware attacks compared to last year, with the number of human-operated ransomware attacks up more than 200 percent since September 2022.

The good news is, for organizations with a strong security posture, the likelihood of an attack succeeding is very low. Typically, an attack is stopped in the pre-ransom phase, with on average 2 percent of attacks progressing to a successful ransomware deployment.

Approximately 40 percent of the ransomware encounters we detected in June were human-driven. Most of these attacks can be attributed to 123 tracked ransomware-as-a-service affiliates. The number of affiliates grew by 12 percent in the last year, setting up conditions for human-operated ransomware attacks to continue to grow in 2024.

**Ransomware breaches per month per 100,000 organizations**

We observed an overall increase in successful ransomware attacks with a sharp decrease in March-April.




Telemetry sources: Microsoft Security Graph, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

### Remote encryption

In a notable change from last year, we observed a sharp increase in the use of remote encryption during human-operated ransomware attacks. Instead of deploying malicious files on the victim device, encryption is done remotely, with the system process performing the encryption, which renders process-based remediation ineffective. On average, 60 percent of human-operated ransomware attacks used remote encryption over the past year. This is a sign of attackers evolving to further minimize their footprint.

### Initial attack vectors

The Microsoft Incident Response team responds to incidents and helps customers secure their most sensitive, critical environments. Based on findings during these engagements, the top three initial access vectors were fairly evenly split, showing criminals are consistently exploiting the same vectors: external remote services, valid accounts, and public facing applications.

We found that among external remote services, adversaries primarily leveraged unsecured remote desktop protocol (RDP) and virtual private networks (VPN). Threat actors attacking valid accounts, where the attacker somehow gained legitimate account credentials, were most often able to log in via Citrix.

Among vulnerable external facing applications, cybercriminals exploited vulnerabilities ranging from zero-day vulnerabilities to those that were two to three years old, with Zoho Java ManageEngine, Exchange, MOVEit, and PaperCut print management software among the top applications exploited.

**Actionable insights**

**To safeguard against these attacks:**

1. It is crucial to implement Zero Trust and least privilege principles.
2. The most efficient solutions are those that can instantly identify attackers by utilizing signals from devices, users, and the entire organization, and take automatic remedial measures across both managed and unmanaged devices.
3. It is essential to have a seamless method to restore encrypted files at the organizational level.

**Additional information**

How automatic attack disruption works in Microsoft 365 Defender | Microsoft

Automatically disrupt adversary-in-the-middle attacks with XDR | Microsoft

# Ransomware targeting

### Unmanaged devices

Most human-operated ransomware attacks attempt to compromise or gain access to unmanaged or bring-your-own devices (personal devices used to access work-related systems and information). These typically have fewer security controls and defenses. We have observed that 80 to 90 percent of all compromises originate from unmanaged devices. Ransomware operators are also increasingly exploiting vulnerabilities in less common software, making it more difficult to predict and defend against their attacks. This reinforces the importance of a holistic security approach.

### Organization size

Despite the notoriety of high-profile attacks last year, the primary victims of ransomware attacks this year were small and medium size organizations. Between July and September 2022, around 70 percent of organizations encountering human-operated ransomware had fewer than 500 employees.

### Industries

While the critical infrastructure sectors experienced the most ransomware encounters this year, cybercriminals have broadly attacked all sectors. Attackers leveraged new techniques as pre-cursors to ransomware to establish the foothold within the victim organization before exfiltration and ransom. As seen in the distribution of pre-ransom notifications sent by Microsoft Defender Experts to our customers, education and manufacturing sectors were key targets. For example, threat actors targeted a critical remote code execution vulnerability found in PaperCut server, which is used by educational organizations.

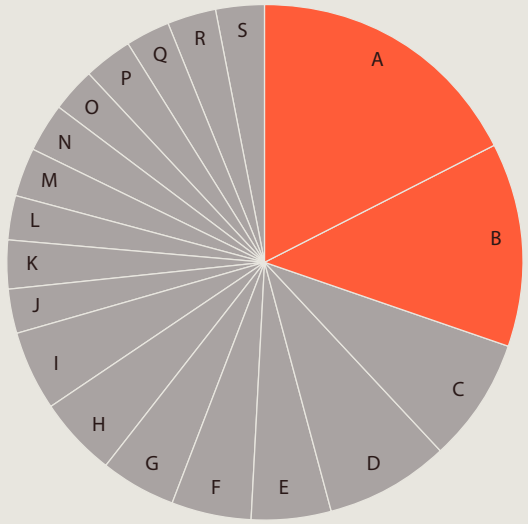
**70%**

of organizations encountering human-operated ransomware had fewer than 500 employees.

**80-90%**

of all compromises originate from unmanaged devices.

**Pre-ransom notifications by industry**




- A Discrete Manufacturing
- B Higher Education
- C Real Estate
- D Professional Services
- E Consumer Goods
- F Retailers
- G Primary & Secondary Edu/K-12
- H IT Services & Business Advisory
- I Insurance
- J Gov Ops & Infrastructure
- K Power & Utilities
- L Media & Entertainment
- M Health Provider
- N Water & Sewage
- O Automotive & Mobility
- P Capital Markets
- Q Medical Manufacturing
- R Automobile
- S Telecommunications

Source: Microsoft Defender Experts notifications

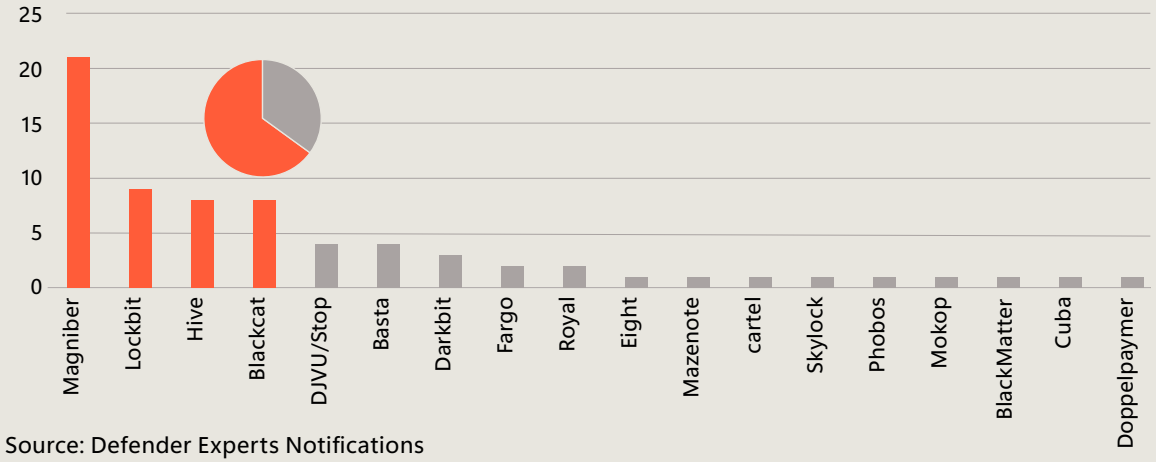
# Ransomware variants

Based on data from Microsoft Defender Experts notifications the top four malware variants—Magniber, Lockbit, Hive, and BlackCat—comprised almost two-thirds of ransomware encounters.

Magniber ransomware, which is an automated variant without human operation, has been linked to Storm-0381, which has a track record of using malvertising, the Magnitude exploit kit, and malicious payloads disguised as Windows updates to disseminate Magniber. Magniber was initially used to target countries in Asia in around 2017, but since resurfacing a few years ago it has expanded its reach to global targets.

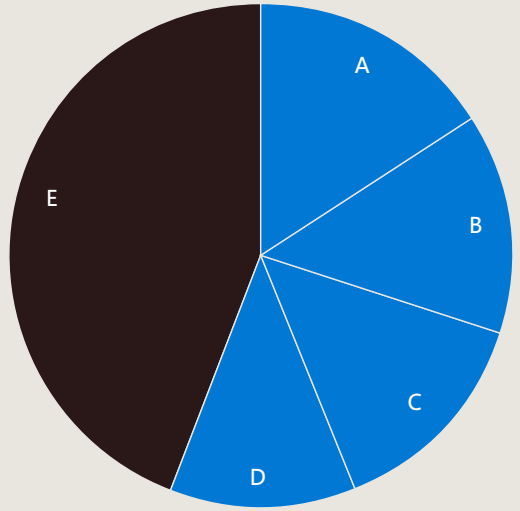
**Breakdown of ransomware by variants**

The top four variants comprised 65% of all ransomware encounters




Source: Defender Experts Notifications

**Top human-operated ransomware variants that achieved breaches**




A 16% Lockbit 3.0

B 14% BlackBasta

C 14% Blackcat

D 12% Royal

E 44% BlackByte
Hive, Play
Akira, BitLocker
Cartel, Cuba
Dagoned
Gazprom
Lorenz
Prestige
Ragnarlocker
Rorschach
Vice Society
Dharma

Source: Microsoft Incident Response

**Human-operated ransomware variants that achieved breaches**

Ransomware accounted for 31 percent of all Microsoft Incident Response customer engagements. Looking at successful breaches among our incident response findings, four human-operated ransomware variants accounted for more than half of all breaches, with Lockbit being the most observed.

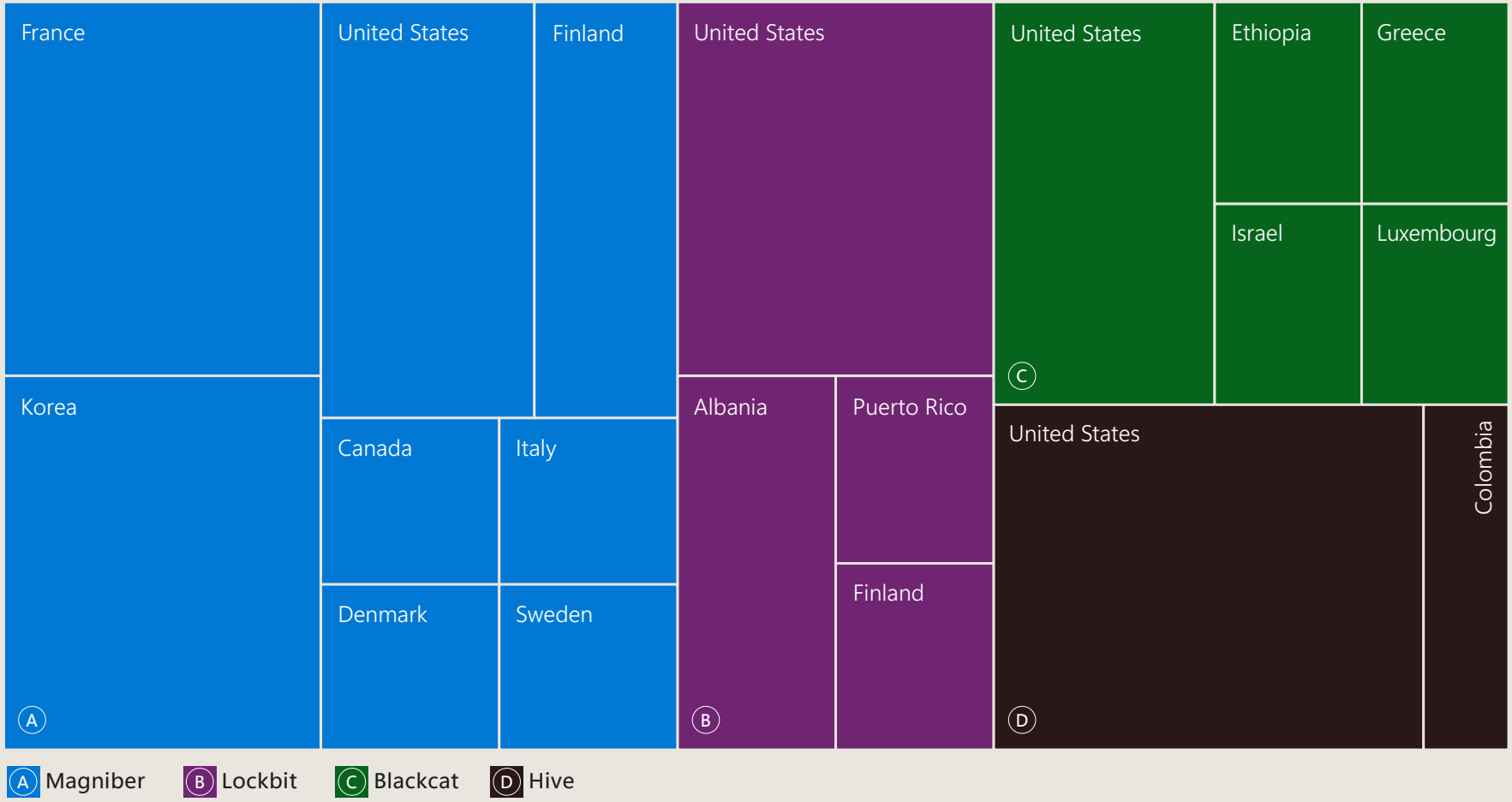
**Ransomware variants** continued

### Regional footprints

The geographical distribution of the Microsoft Defender Experts notifications reveals that the top ransomware variants had varying regional footprints. This reflects the targeted nature of attacks by their operators.

**Countries targeted by the top four ransomware variants**

The regional presence of ransomware was an indication of targeted attack and encryption by the threat actors.




Source: Microsoft Defender Experts notifications

# How cybercriminals are using remote monitoring and management tools

Attackers continue to abuse legitimate remote monitoring and management (RMM) software for post-compromise activity such as information-stealing and delivering malicious payloads like ransomware. Microsoft incident responders found that 17 percent of intrusions involved known RMM tools.

**17%**

of intrusions involved known RMM tools.

In addition to providing attackers with persistent access to compromised systems, RMM software allows significant permissions that enable attackers to launch PowerShell commands or run scripts with system-level privileges. Threat actors can also abuse RMM software to copy files to a clipboard and exfiltrate data using a file transfer web service.

Because managed service providers, IT support, and system administrators use RMM software for legitimate purposes, it is often permitted by application controls. This makes automated detection of its use in an attack difficult. Its presence often blends in with common activity, buying the attacker time and complicating incident response as defenders may overlook the software. Organizations that do not use RMM software can defend against its abuse during an attack by using application control policies or perimeter network blocking rules.

**Actionable insight**

1. If your organization does not use RMM software, you can protect against its abuse during an attack by implementing application control policies or perimeter network blocking rules.

# Spotlight on cryptojacking

Cryptojacking is the unauthorized use of other people's devices to mine cryptocurrency. It generally does not trigger an incident response; rather, the criminal activity is often detected while investigating a separate incident. We observed evidence of current or past coin mining activity in 4.2 percent of all our engagements during the year. In these incidents, responders identified the presence of XMRig mining malware or the creation of virtual machines within a customer's subscription for coin mining.

Cryptojacking slows down an infected device, uses its resources, can steal information, and decreases overall performance.

Microsoft Defender Experts has identified the following Linux hosted application vulnerabilities being exploited for cryptojacking:

**Additional information**

Cryptojacking: Understanding and defending against cloud compute resource abuse | Microsoft

| Applications exploited by cryptojacking gangs | Publicly disclosed security flaws in the list of Common Vulnerabilities and Exposures (CVEs) |
|---|---|
| Teclib GLPI | CVE-2022-35914 |
| PACS (picture archiving and communication system) | Not applicable |
| Apache NiFi | Not applicable |
| Liferay portal | CVE-2020-7961 |
| Oracle WebLogic | CVE-2020-14750<br>CVE-2020-14882<br>CVE-2020-14883 |
| Confluence | CVE-2022-26134 |
| WSO2 | CVE-2022-29464 |
| GeoServer | Not applicable |

# Insights on data exfiltration

Data exfiltration involves the unauthorized removal or movement of data from a device. Since November 2022, we have observed a doubling of potential data exfiltration instances after threat actors compromised an environment. This growth is consistent with the rise in double and triple extortion activity after ransomware attacks that we and the broader security community have observed in the past several years.

Not all data theft is associated with ransomware; it can also be part of credential harvesting or nation-state espionage. Stopping data exfiltration therefore requires a broader approach than focusing solely on preventing ransomware payload deployment and backup deletion.

### Infostealers

Information stealers (infostealers) are malicious software designed to steal data stored in browsers. Such data includes session tokens and cookies which can include multifactor authentication (MFA) claims, saved passwords and input form data, credit card information, user files, and cryptocurrency wallets. They can also harvest credentials for internet-facing systems and applications including VPN, RDP, virtual desktop infrastructure including Citrix, and identity providers such as Azure Active Directory and Okta.

In some instances, infostealers act as loaders for other malware.

As infostealers have become more prevalent in the last two years, they have increased as a risk to enterprise security. For example, an unmanaged device might lead to corporate compromise after an employee syncs their workplace credentials with infected home devices from browsers that are signed in.

Infostealers are advertised as a malware-as-a-service offering. The infostealer ecosystem is a multi-tiered business model usually involving three or four entities:

- The developer/operator develops the malware, operates its infrastructure, and sells the malware build to multiple distributors.
- The distributor uses the build to create infostealer payloads, deploys the infostealer in phishing or malvertising campaigns, downloads the infostealer output from the operator's centralized infrastructure, and is responsible for getting customers and developing a monetization strategy, which usually includes posting the output onto online credential marketplaces.
- The credential marketplace advertises stolen credentials for purchase. These online forums include Russian Market, Genesis Market, and Industrial Spy Market.
- The customer purchases infostealer output from the distributor or credential marketplace.

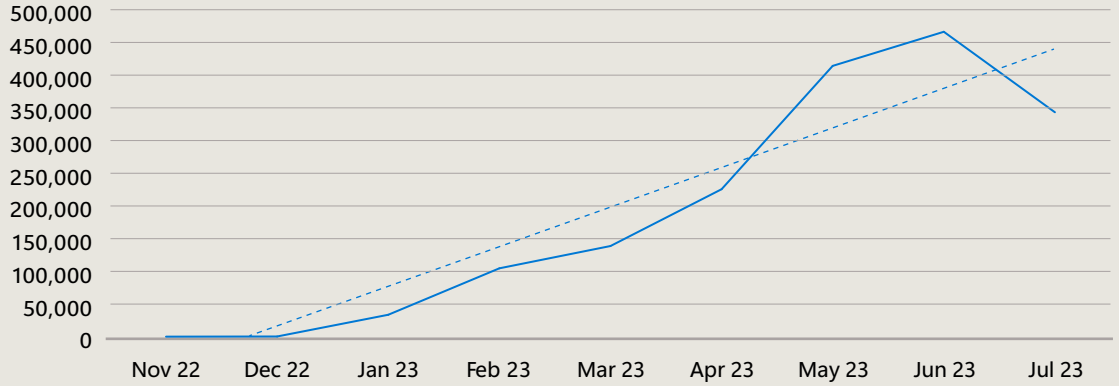
The infostealer ecosystem has enabled a new group of threat actors that leverage these tools to exfiltrate data and destroy resources. Such threat actors include Karakurt, the now-inactive Strawberry Tempest (DEV-0537, formerly LAPSUS$), Storm-0875 (0ktapus), Storm-0829 (Nwgen Team), Storm-0744, and Storm-0971.

### Data extortion

Ransomware operators have multiple opportunities to monetize their attacks, all of which are linked to data–encrypting, deleting, or publishing it. Because of the sensitivity of many organizations' data, some threat actors have turned to exfiltrating data for ransom without ever deploying an actual ransomware payload. Microsoft has observed that while approximately 16 percent of recent successful human-operated ransomware attacks involved both encryption and exfiltration, 13 percent used exfiltration only.

To exfiltrate data, attackers often leverage open-source data management and synchronization tools such as Rclone and MEGAsync. These tools are freely available for legitimate purposes and allow large volumes of data to be uploaded to remote cloud resources. Given that many RaaS programs include a suite of data extortion support offerings—including leak site hosting, payment pressure, and cryptocurrency transaction services—it is easier than ever for cybercriminals to monetize data exfiltration.

**Instances of potential exfiltration**




Sources: Microsoft Defender for Endpoint, Microsoft Purview Data Loss Prevention, Microsoft Defender for Office 365, Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft 365 Defender, App Governance in Microsoft Defender for Cloud Apps, Microsoft Sentinel, Azure Active Directory Identity Protection.

# Disrupting the financial networks of cybercriminals: a hypothetical case study

One of the best ways to deter cybercriminals is to hit them where it hurts: in their wallets. The Microsoft Digital Crimes Unit (DCU) has been doing that through a holistic strategy which places financial disruption at the core of its investigations.

Going after the financial networks of cybercriminals means leveraging advanced analytics and tools to identify bad actor assets, working with public and private sector partners, and scaling the use of traditional and new legal approaches to disrupt the financial flows of the cybercrime ecosystem. Here's what that might look like:

Microsoft identifies a suspected ransomware attack and proactively contacts the impacted customer. The customer confirms its files were encrypted and that it received a ransom demand to be paid to a cryptocurrency wallet. Microsoft works with the victim on incident response while the DCU analyzes the attacker and their virtual wallet. Using tools provided by industry partners who specialize in analyzing cryptocurrency transactions, the DCU identifies more of the threat actor's wallets and technical details of their communications.

With the victim's permission, Microsoft uses its membership in the National Cyber Forensics and Training Alliance (NCFTA)—a non-profit organization that unites industry and government partners to combat cybercrime—to share this information quickly and securely. The group confirms the actor is a known ransomware group and provides details including other wallets and infrastructure the cybercriminals use.

Op Pa Cybersecurity Tech Accord principles mapping index on **page 124**

Against the recommendation of law enforcement, the victim may determine that they must pay the ransom because of the critical nature of the encrypted data and their lack of back-ups. Based on the work of the DCU and its NCFTA partners however, the company decides to coordinate payment with law enforcement. After the victim pays, law enforcement tracks the funds and works with cryptocurrency exchanges to freeze the cryptocurrency before the ransomware group can withdraw it.

Law enforcement then returns the money to the victim through the appropriate legal process. Additional investigations may lead to the arrest and prosecution of the criminals.

Given the complexity and global nature of ransomware attacks and other cybercrime activity, this collaborative approach is necessary to disrupt the finances of criminals, at scale. Microsoft and the DCU are leading efforts with partners and will continue to develop technology and legal approaches to bring threat actors to justice.


Microsoft Digital Crimes Unit

# Collaboration to disrupt the ransomware business model

One recommendation of the Ransomware Task Force (RTF), of which Microsoft is a part, is to disrupt the ransomware business model and decrease criminal profits. In pursuit of this goal, the Institute of Security and Technology (IST) mapped the ransomware payment ecosystem in 2022.

**Additional information**

Mapping the Ransomware Ecosystem | Institute for Security and Technology

The Ransomware Task Force (RTF) unites key stakeholders across industry, government, and civil society

This groundbreaking identification of the actors, processes, and information involved in the ransomware payment ecosystem illuminates how the ransom payment moves from the victim to the ransomware actor to be obfuscated, cashed out, and reinvested.

The laundering process spans cryptocurrency companies, virtual asset service providers (VASPs), peer-to-peer and cryptocurrency exchanges, mixers, merchant services, and dark net markets, among other entities. IST found that previously un-leveraged information is produced as a ransom payment moves through the chain. This information can be accessed and potentially shared by a range of entities including, but not limited to, antivirus vendors, cloud service providers, hosting providers, cryptocurrency exchanges, and tooling providers. Efforts coordinated by the RTF and NCFTA, among others, can also use this information to add friction to–and potentially disrupt–the ransomware payment ecosystem. The ultimate goal is to disincentivize the use of ransomware by making it harder for ransomware operators to successfully collect on their attacks.

# Defending against future ransomware trends

As of May 2023, 92 percent of the RTF recommendations for combatting ransomware had been actioned in some way, with 50 percent experiencing significant progress, including through legislation and policy adoption.[1] Just as defenders are innovating, however, ransomware operators are too. As a result, Microsoft is focused on understanding how ransomware activity may develop over the next few years to proactively counter it. Going forward, we expect cyber criminals will seek to leverage automation, AI, and hyperscale cloud systems to scale and to maximize the profitability of ransomware attacks. Organizations looking to minimize their vulnerabilities to these approaches must respond by modernizing their organizational skills, mindset, approach, and technology.

**Actionable insights**

1. Modernize cybersecurity skills: Use AI to augment human cyber defense skills and capabilities for organizations and for collective defense. AI can also be used to expedite the time to detect and respond to ransomware attacks.
2. Modernize mindset: Organizations should understand the benefits of innovations in the public cloud, which includes hyper-scalability cybersecurity capabilities, to protect digital platforms from cybercriminals and nation-state attackers.
3. Modernize approach: Cybersecurity can no longer be seen as a technical problem; for greater resilience it must be seen as an organizational risk by leaders in the organization and managed accordingly.
4. Modernize approach: Legacy technology and siloed standalone security products are not efficient or effective at defending against sophisticated cyber attackers. Organizations should invest in integrated cybersecurity platforms that share signals across the digital backbone to provide end-to-end visibility and inform defenders across an organization's surface attack area.

# What is the Optimal Ransomware Resiliency State?

Microsoft's mission to keep ourselves and our customers safe from ransomware continually evolves and grows. A resilient defense is particularly important as ransomware operators increasingly shift toward hands-on-keyboard attacks that enable sophisticated cybercriminals to seek out and exploit vulnerabilities.

Op Cybersecurity Tech Accord principles mapping index on **page 124**

Despite developments in the ransomware space, the overall approach of our Ransomware Elimination Program remains the same: to deter or counter ransomware attacks by removing opportunities for financial gain by threat actors.

In last year's report, we introduced our two-pillar approach to ransomware, with dedicated initiatives to support our enterprise and our customers. This year, our efforts resulted in three key outcomes:

- **Continuous improvement for business continuity and recovery**: We emphasized the role of employees in our defense strategy through tabletop exercises and rigorous simulations to verify our protective capabilities, supported by training for excellence in incident response preparedness.
- **Advanced evaluation of ransomware-specific controls**: Integrating new methodologies, we developed a ransomware-specific technology evaluation program to ensure controls meet the requirements of our enterprise.
- **Improved feedback loops**: We streamlined engagement between our security operating center and the product groups that build the security tools that Microsoft and its customers rely on. This provided richer insights with more actionable data and improved our ransomware protection and detection capabilities in the products and services we used.

Over the coming year, we will continue to iterate and develop our processes to further reduce the risk of ransomware impact on our environment.

### How we can build resilience against ransomware

Our approach aims to ensure that our internal products, services, and teams—including those supporting our customers—will be best positioned to defend against ransomware attacks today and in the future.

To optimize resilience, we conducted an internal assessment using the National Institute of Standards and Technology's published framework for managing the risk of ransomware (NIST.IR.8374). Based on the results, and in conjunction with data and observations of real-world human-operated ransomware, we have established a comprehensive set of requirements across different technology domains to defend against ransomware attacks. We call this our Optimal Ransomware Resiliency State (ORRS).

Integrating what we have learned from our Zero Trust journey, ORRS consists of 40+ requirements that span myriad aspects of the security landscape, from policy and governance to infrastructure and data. The requirements are platform agnostic to ensure compatibility with any device that we mandate and include employee training, and ensuring business continuity and data accessibility.

Pr Op Em Cybersecurity Tech Accord principles mapping index on **page 124**

We believe that ransomware resiliency should be available to all organizations, regardless of size or industry. Over the coming months, we're focused on the implementation experience of ORRS with new, streamlined requirements that ensure resiliency and performance are not compromised.

### The five foundations of the ransomware elimination journey

We have identified five foundational principles which we believe every enterprise should implement to defend against ransomware. When fully implemented, the Foundational Five provide proven defenses across identity, data, and endpoints. While we make exclusive use of our first-party products, the Foundational Five are solution-agnostic if they are properly implemented and fully enabled.

### The Foundational Five

1. Modern authentication with phish-resistant credentials
2. Least Privileged Access applied to the entire technology stack
3. Threat- and risk-free environments
4. Posture management for compliance and the health of devices, services, and assets
5. Automatic cloud backup and file-syncing for user and business-critical data

Pr Em Cybersecurity Tech Accord principles mapping index on **page 124**

**What is the Optimal Ransomware Resiliency State?** continued

A threat- and risk-free environment is defined as an environment protected by proactive measures—through tools and technologies—to prevent ransomware. These include malware detection, endpoint detection and response, vulnerability management, security operations center enablement, the enforced blocking of unhealthy devices, and brute-force protection for operating systems.

**Links to further information:**

Building an anti-ransomware program | Microsoft

Why Microsoft uses a playbook to guard against ransomware | Microsoft

Microsoft Security Ransomware incident response playbook framework

### Actionable insights

1. Understand your security risk relative to the Foundational Five. Ensure all features are fully turned on and active since, when combined, these make for a strong defense network.
2. Prioritize protective controls while ensuring you have the detective capabilities ready to identify new threats and risks in your environment.
3. Test and verify the effectiveness of implementations for your business needs. You may find unexpected gaps in your ransomware armor that need addressing.
4. Continuously improve your process for responding to and recovering from attacks and for practicing incident response readiness. Tabletop exercises and cross-company involvement are particularly useful.
5. If you do not already have one, consider building an incident response plan that covers specific ransomware scenarios for all major areas to ensure business continuity.
6. Consider using the hyperscale cloud as a venue where these principles are accessible quickly with low cost and low complexity.

# A call to action

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in disrupting the cybercriminal economy.

1. Focus on user identity, device health, and access control to prevent lateral movement and privilege escalation in the network.
2. Implement a Zero Trust approach to reduce the attack surface and improve resilience against cyber threats. By adopting this model, organizations can increase the cost to attackers and limit the impact of successful intrusions, thus reducing the blast radius.
3. Keep cybersecurity fundamentals up to date and leverage cloud-based tools for faster threat detection and response.
4. Establish a ransomware defense strategy to mitigate the impact of extortion attacks that are becoming more frequent and damaging. Implementing a plan should be a priority especially because of the near certainty that an organization will experience at least one attack in the next few years.

**Additional information**

Advancing Modern Strong Authentication | Microsoft

How to configure for ransomware prevention in your organization | Microsoft

Stop attack progression with automatic disruption of ransomware and BEC attacks | Microsoft

# Insights on phishing

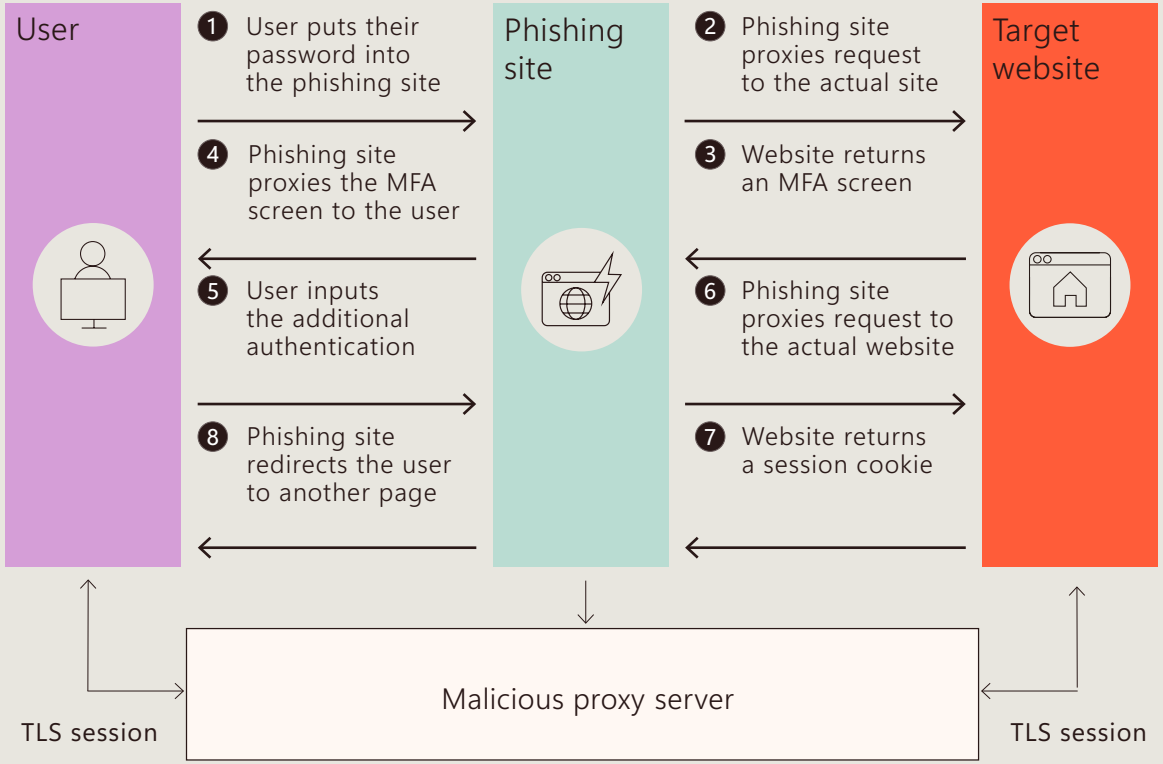
## Adversary-in-the-middle phishing attacks

Adversary-in-the-middle (AiTM) is a longstanding technique used by threat actors to obtain credentials, session cookies or personal data, or to distribute malware.

We have consistently observed a daily influx of high-volume AiTM phishing campaigns, with some instances involving millions of phishing emails sent within a 24-hour period. This trend of high-volume campaigns first appeared in September 2021 and we saw a significant surge in mid-July 2022, indicating an effort to bypass MFA on a massive scale. Unlike traditional phishing attacks, revoking and resetting user account credentials is not enough to address AiTM phishing incidents. The stolen session cookies also need to be revoked because session cookies, which are data stored in browsers, grant privileged access without repeated authentication.

During an AiTM phishing attack, a reverse proxy server is set up between the target and a legitimate login page. Reverse proxy servers sit between a client, such as a web browser, and a web server, forwarding information and requests between the client and the server. Reverse proxies are used legitimately for increasing security and performance but can also be used for malicious purposes such as AiTM attacks. The target unwittingly submits their credentials through the proxy, which triggers an MFA prompt on their mobile device. After the user inputs the authentication code, the proxy continues to deceive them by presenting subsequent MFA screens, relaying the user's input and allowing the attacker to access the account without the user's knowledge.

Anatomy of an AiTM phishing attack



**Adversary-in-the-middle phishing attacks** continued

In AiTM, the target is presented a replica or imitation login page, as in traditional phishing methods. However, a separate server controlled by the threat actor or phishing service is used to submit the stolen credentials to the legitimate login service, triggering an MFA prompt. The phishing infrastructure then displays a copy of an MFA screen to the target. This is distinct from AiTM over reverse proxy, as no HTTP packets are proxied between the target and the login service.

Microsoft tracks multiple threat actor groups associated with prominent AiTM phishing kits and services and one prolific threat actor using multiple AiTM phishing services to carry out high volume phishing campaigns. These prominent kits/services are known as Caffeine (attributed to Storm-0867), EvilProxy (attributed to Storm-0835), and NakedPages (attributed to Storm-1101). We have also observed AiTM phishing campaigns linked to tracked but unidentified kits or services.

$200-$1000

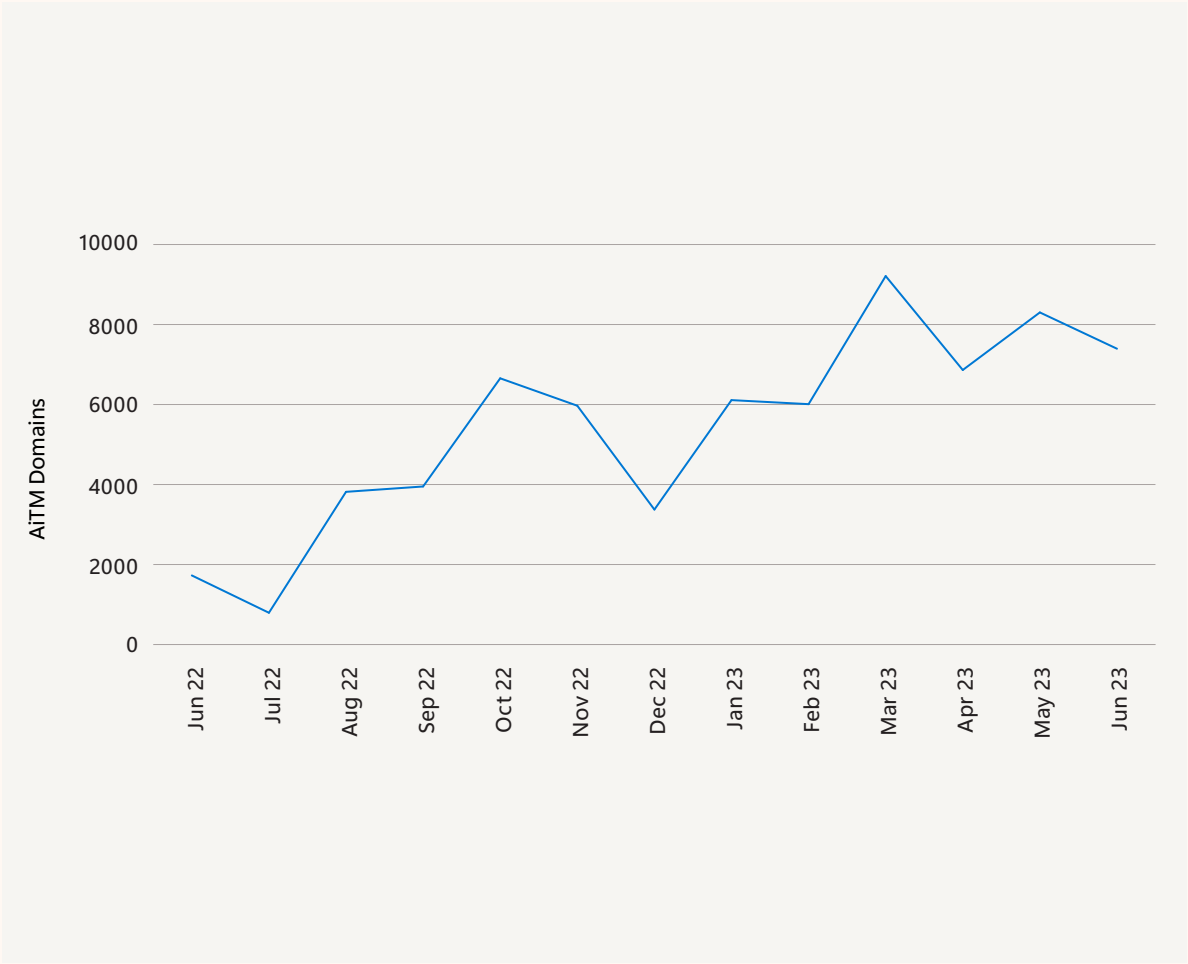
Monthly licensing fees paid by cybercriminals to carry out daily phishing campaigns.

While other kits–such as Evilginx2, Modlishka, and Muraena–have been available for free in open sources for years, they lack the service and support offered by paid-for kits. As a result, the addition of AiTM phish kits to phishing-as-a-service has supplied advanced phishing capabilities to a wider range of threat actors, reduced entry barriers, and enabled more effective attacks.

Caffeine, EvilProxy, and NakedPages each have hundreds of customers. These cyber criminals pay monthly license fees ranging from $200 to $1,000 USD and carry out daily phishing campaigns. Because so many threat actors use these services, it is impractical to attribute campaigns to specific actors. Instead, we track these phishing services, block phishing activity from them, and work to provide effective detection and defense for customers.

**AiTM domains growing as attacks become more common**

The number of domains that we tracked leading to AiTM phishing pages grew consistently throughout the last 12 months




Source: Microsoft Defender for Office 365

# Evolving phish techniques

Phishing campaigns continue to improve in sophistication, including leveraging genuine services or websites and tailoring phishing links for individual users. By simulating user interaction in virtual machines, we can analyze untrusted files and URLs to assess their safety. The main goal is to deliver speedy and accurate verdicts on content.

Examples of what we're seeing in real-time analysis:

- **Emails sent from trusted third parties.** Attackers send phishing emails to all the contacts of their victims and then respond on the email thread with specially crafted messages and a malicious URL.
- **Emails with legitimate URLs.** Attackers host phishing URLs on legitimate cloud service providers such as Adobe, Dropbox, Google, and Microsoft. After multiple redirects, victims are led to the final landing page, which steals credentials or downloads malicious payloads onto their machine. Given these are popular services, it is difficult to distinguish malicious links from genuine ones.
- **OneNote malware.** Attackers abuse OneNote to execute malicious software. Phishing campaigns observed by Microsoft Defender Experts include OneNote attachments, URLs leading users to download OneNote attachments, and PDFs containing URLs that led to OneNote malware downloading.
- **OAuth device code phishing.** The attacker generates a user code, then creates a phishing email with it and a link to provide the code. This allows the attacker to sign-in on behalf of the user.
- **Other targeted phishing attempts.** Our experts also observed targeted phishing attempts in which attackers identified user-specific details through social engineering, then created tailored phishing campaigns using look-alike domains to which the users have subscribed, with contents matching the users' interests. This significantly increases the success rate of a compromise attempt.

**10,000**

In April-June 2023 we alerted users of approximately 10,000 password entries per month into malicious sites.

Source: Enhanced Phishing Protection with Microsoft Defender SmartScreen, across third-party browsers running on Windows 11

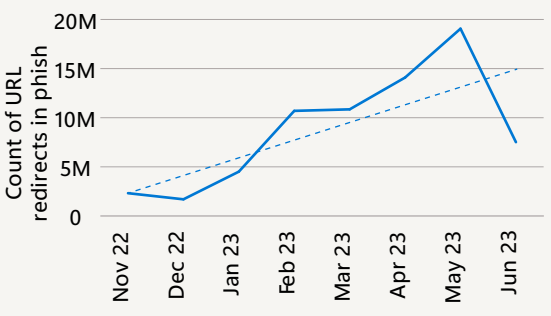
# Trends in file entities used in phish

Using data from Microsoft Defender for Office 365, we observe trends in file entities that are commonly used in phishing attacks. HTML files are often used for creating fake web pages that trick users into divulging personal information. PDF files can exploit a user's trust by embedding malicious links or using social engineering tactics to persuade users to open attachments that execute malware. URLs are commonly used to deceive users into visiting fraudulent websites.

This year, we observed major attack patterns involving URLs with open redirectors and open shorteners being dominant attack vectors.

URL open redirectors are vulnerabilities found in web applications that enable attackers to manipulate URLs to redirect unsuspecting users to malicious websites. Here, they may be victim to phishing attacks, data breaches, account takeovers, or malware infections.

### URL redirect abuse on the rise

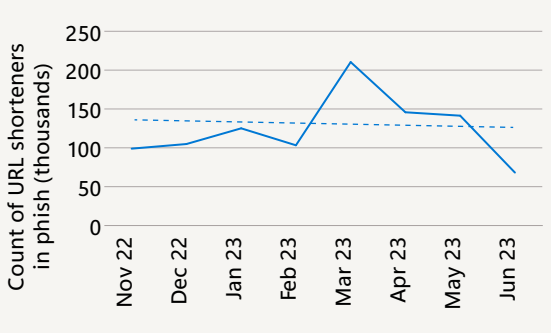



Source: Microsoft Defender for Office 365

Malicious actors can use URL shorteners in tandem with URL redirectors to send users to harmful websites or deceptive phishing pages.

Use of URL shorteners spiked in March, but remained constant overall.

### Prevalence of URL shorteners




Source: Microsoft Defender for Office 365

# Analyzing click behavior in phishing simulations

Phishing campaigns continue to improve in sophistication, including leveraging genuine services or websites and tailoring phishing links for individual users. By simulating user interaction in virtual machines, we can analyze untrusted files and URLs to assess their safety. The main goal is to deliver speedy and accurate verdicts on content.

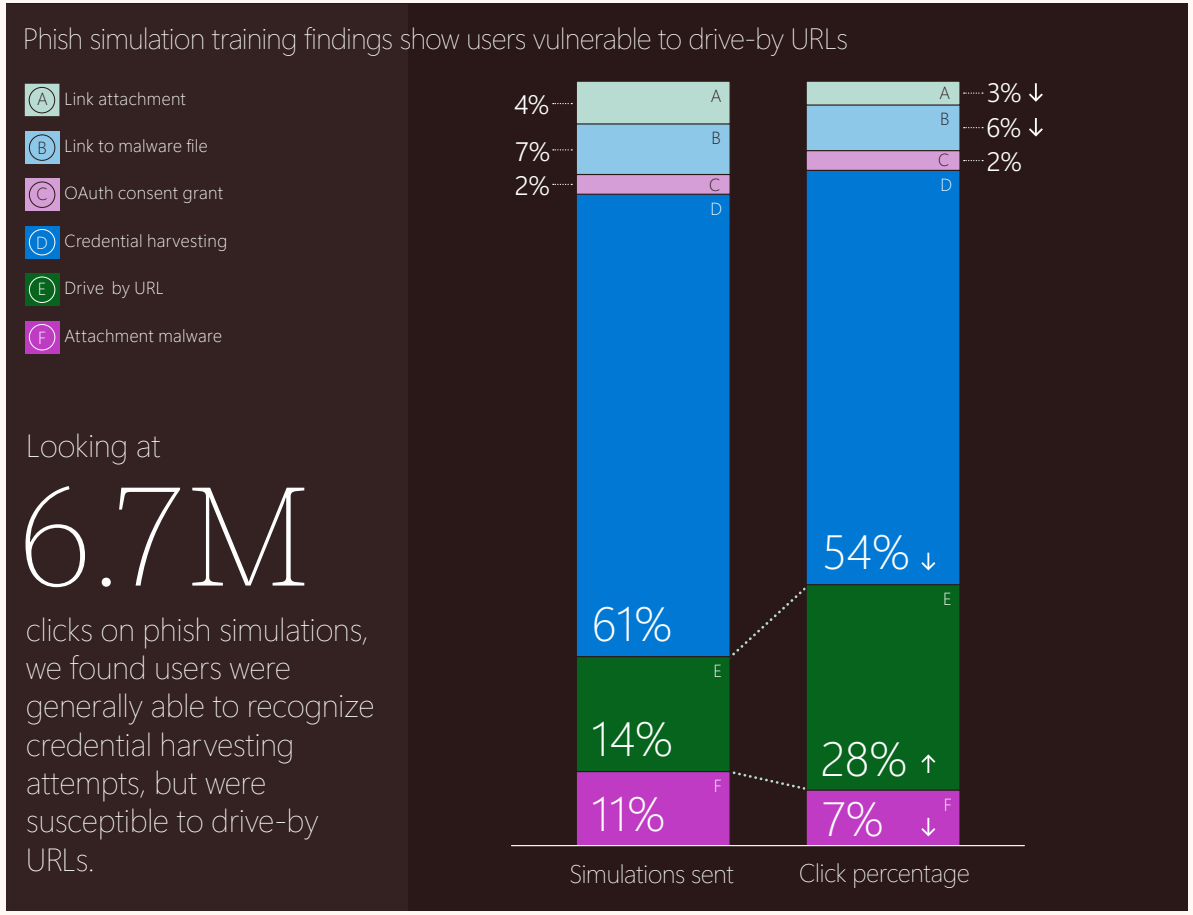
The fundamentals of phishing haven't changed over time; approximately 90 percent of phishing attacks involve social engineering. This is primarily conducted through email that leads the victim to reveal sensitive information, click a malicious link, or open a malicious file. Phishing attacks are cost-effective for attackers, adaptable to evade prevention measures, and boast high success rates. Compromise rates range from single digits to 40 percent, influenced by a wide range of variables from simulation difficulty to user type. We evaluated attack simulation training data from tens of millions of users to gain insights into the impact of phishing training.

### Why is phishing such a challenge?

Humans remain the primary risk vector in social engineering attacks. At the same time, phishing attack mechanisms are constantly evolving, and bad actors create new tactics. Users often click on links and attachments by habit and without conscious consideration of their actions, thereby opening the door to cybercrime. Three factors explain why users remain a key vulnerability:

1. As threat tactics rapidly evolve, technical systems will not be able to completely prevent social engineering attacks and human behavior will persist as a vulnerability for attackers to manipulate.
2. While security awareness programs, designed to help users identify social engineering attacks and respond appropriately have some success, often it is not the user's lack of knowledge that drives phishing susceptibility.
3. So far, users have not demonstrated the ability to consistently change their behavioral risk tendencies enough to show measurable improvement against an ever-evolving threat landscape.

Users are particularly vulnerable to drive-by URL attacks. These involve simple link-clicks that take victims to websites that collect telemetry or entice the user to a downstream attack. Whereas a credential harvest attack involves two clicks—one to get to the credential harvesting page and another to enter the credentials—a drive-by requires just one click. Drive-by URL attacks are usually less impactful, but many organizations use them to measure their click susceptibility.




Source: Microsoft Defender for Office 365, attack simulation training data

### How video-based trainings alone fall short

Most enterprise phishing awareness programs prioritize meeting training compliance requirements over delivering effective behavior change programs. They operate under the misguided assumption that periodic exposure to simulated phishing attacks, accompanied by a brief educational encounter (typically in the form of a narrated video with limited interactive elements), will equip users to be able to identify and avoid advanced and evolving phishing attempts. However, these programs have proven to be fundamentally flawed.

Although tens of millions of computer users have taken phishing training, we have found that phish clicking behavior is reduced by employing video-based training by about three percent, at best. This number has remained remarkably stable over the years. Based on this data, we conclude that video-based training is not an effective way to reduce an organization's phish susceptibility.

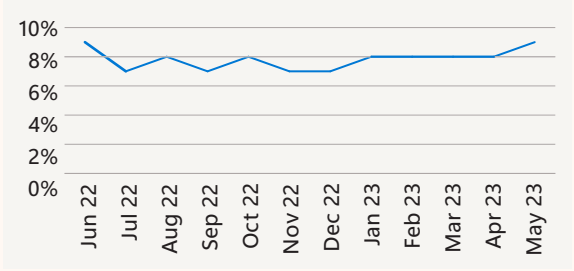
### Tailored approaches are needed

The security awareness and training industry is beginning to adopt objective behavioral measures and contextual experiences that prioritize behavior change over information delivery. This involves tailoring the approach to individual users. We believe this approach holds the greatest potential for reducing behavioral risk against modern social engineering attacks. Under this approach, organizations must embrace a new perspective regarding the involvement of their users in thwarting attacks and conduct innovative experimentation with user engagement strategies.

To truly tackle the issue of phishing, it's important to recognize that every user is unique and has their own behavioral tendencies. Our phishing awareness programs go beyond generic, one-size-fits-all training and instead provide tailored and context-aware engagement models that can be implemented at scale. We understand that each user requires a personalized learning experience based on their unique behaviors and profile, such as job function, security posture, and past actions. For example, our phish simulations are tailored to each user's performance based on telemetry from previous simulations sent. Providing personalized learning experiences based on each individual's unique behaviors and profile can enable organizations to make a real impact in reducing phish susceptibility.

### Percentage of clicks on phish simulations

Link-clicking behavior by users has remained relatively unchanged despite the widespread implementation of security awareness training programs, and increased sophistication of phish.



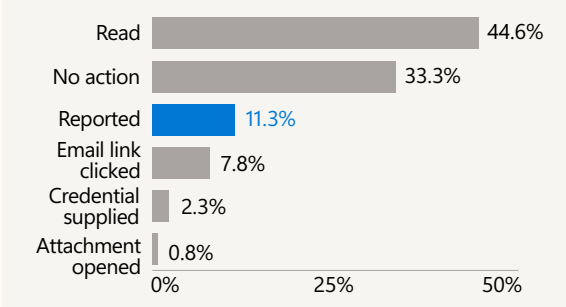

Source: Microsoft Defender for Office 365 attack simulation training data

### Inaction is better than clicking, but reporting is the best action to take.

Reporting phishing attempts is crucial to prevent cyberattacks. Users can help security teams identify and block malicious emails, websites, and other threats. However, only 11.3 percent of users who receive phishing emails report them, despite 89 percent refraining from clicking on links or opening attachments.

Administrators can use awareness campaigns, teaching guides, and rewards to raise awareness of phishing campaigns and encourage consistent reporting behavior. There is a genuine opportunity for organizations to prioritize enhancing user reporting consistency, as current rates fall short of potential.

### User responses to phish attempts still insufficient




**Over the past six months, we found users reported phishing attempts only 11.3% of the time. While no action is better than clicking, reporting phishing attempts would be best to help security teams identify incoming threats.**

Source: Microsoft Defender for Office 365 attack simulation training data

Employees must also know how to recognize and respond to evolving phishing techniques. Additionally, emphasis should be placed on strengthening organizational resiliency, such as through Zero Trust strategies which isolate and contain the potential impacts of phishing.

#### Additional information

Attack Simulation Training: New insights into targeted user behavior

Simulate a phishing attack with Attack simulation training | Microsoft Learn

#### Actionable insights

**To safeguard against these attacks:**

1. Shift phishing training programs away from being compliance oriented to more proactive, behavior change focused.
2. Develop tailored and context-aware education models that treat users as distinct individuals and can be implemented at scale.
3. Teach users that reporting is a gold standard behavior in protecting their enterprise.
4. Treat phishing education programs as part of a broader Zero Trust organizational resiliency strategy.